Wolters Kluwer

GDPR PRODUCTFICHE

Fiscale Simulaties

1. Aard van de Verwerking

Deze suite bestaat uit aantal tools die (fiscaal) advies geven op basis van beperkte invoer, er wordt een rapport gemaakt, er is geen opslag van data.
Ook in deze suite is een tool opgenomen voor het opstellen van een Financieel plan. Dit is een wettelijke vereiste en de tool volgt de geldende wetgeving. Tevens worden er resultaten getoond en kan er een rapport worden aangemaakt.

2. Categorieën van Persoonsgegevens die verwerkt worden

Verwerker zal uitsluitend volgende categorieën van Persoonsgegevens verwerken in het kader van dit Addendum:

☒ identiteitsgegevens (naam, adres, gsm, e-mail, geboortedatum, nummerplaat, IP-adres, …)
☒ contactinformatie (adres, e-mail, IP-adres, IMEI, …)

Bijzondere Categorieën van Persoonsgegevens met betrekking tot:

Niet van toepassing.

3. Categorieën van Betrokkenen

☒ klanten van Verantwoordelijke
☒ eigen werknemers Verantwoordelijke

4. Doeleinden van de verwerking

☒ boekhoudkundige en juridische verplichting

In het kader van onze voortdurende inspanningen om de kwaliteit en functionaliteit van onze software/product te verbeteren, verzamelen en analyseren wij gegevens over het gebruik van onze producten. De verzamelde gegevens worden uitsluitend gebruikt voor de volgende doeleinden:

- Identificeren en oplossen van technische problemen en bugs
- Optimaliseren van de gebruikservaring en interface
- Ontwikkelen van nieuwe functies en verbeteringen die zijn afgestemd op de behoeften en voorkeuren van de gebruiker
- Uitvoeren van algemene productanalyse om de efficiëntie en effectiviteit van de software te verbeteren

5. Retentieperiode

Persoonsgegevens zullen verwerkt en bijgehouden worden gedurende volgende periodes:

- Ingevoerde Persoonsgegevens: persoonsgegevens worden bijgehouden voor de duurtijd van de Overeenkomst en tot drie maanden na het einde van deze Overeenkomst;
- Persoonsgegevens via helpdesk support: tot 3 maanden na einde van de Overeenkomst.

©Legal Office WKB

6. Beveiligingsmaatregelen

Technische en organisatorische maatregelen kunnen worden beschouwd als de stand der techniek op het moment van sluiten van de Overeenkomst van Dienstverlening. Verwerker zal technische en organisatorische maatregelen na verloop van tijd evalueren, daarbij rekening houdend met kosten voor doorvoering, aard, omvang, context en doelstellingen van verwerking, en het risico van verschillen in de mate van waarschijnlijkheid en ernst voor de rechten en vrijheden van natuurlijke personen.

©Legal Office WKB

Gedetailleerde technische en organisatorische maatregelen:	
Toegangscontrole: gebouwen	Toegang tot de gebouwen waar informatiesystemen zijn geplaatst, worden door zowel technische als organisatorische maatregelen gecontroleerd (informatiesystemen van Microsoft Azure).
Toegangscontrole: systemen	Toegang tot netwerken, operationele systemen, user administratie en applicaties vereisten de nodige autorisaties: geavanceerde paswoord procedures, automatische time-out en blokkering bij foutieve paswoorden, individuele accounts met historieken, encryptie, hardware en software firewalls.
Toegangscontrole: gegevens	Toegang tot gegevens zelf wordt beheerst door organisatorische maatregelen: user administratie en user accounts met specifieke toegang, opgeleid personeel omtrent gegevensverwerking en veiligheid, scheiding van de operationele systemen en de testomgevingen, toekennen van specifieke rechten en bijhouden van historieken van gebruik (aanwezigheid van een audit-trail), toegang en wissing.
Encryptie van gegevens:	in transit: https in rust: Data-opslag wordt transparant geëncrypteerd
Vermogen om blijvende vertrouwelijkheid, integriteit, beschikbaarheid, en veerkracht van verwerkingssystemen en -diensten te garanderen:	Scheiding van productie- en testomgeving, scheiding van specifieke gevoelige gegevens, automatische back-up, geavanceerde paswoordprocedures, specifieke gebruiksrechten, bijhouden van historiek.
Vermogen om de beschikbaarheid van en toegang tot de Persoonsgegevens tijdig te herstellen in het geval van een fysiek of technisch incident:	Wolters Kluwer beschikt over een disaster recovery strategy.
Proces voor regelmatig testen, beoordelen en evalueren van de doelmatigheid van technische en organisatorische maatregelen om de veiligheid van de verwerking te garanderen:	- Software scans op code en third party libraries - Thread modeling - Pen tests - Security audits cf. Global WK Security
Beschikbare certificering:	- ISO/IEC/ 27001 certification
Andere:	/

©Legal Office WKB

7. Subverwerkers

Volgende Subverwerker(s) voeren in opdracht van Wolters Kluwer dienstverlening met betrekking tot persoonsgegevens uit:

Naam	Adres	Doel van gebruik
MicrosoftCorporation (Azure) - Microsoft NV	Brussels National Airport - Passport Building 1K Luchthavenlaan	Uitvoering van de gebruikersovereenkomst, onderhoud en ontwikkeling van het platform.

8. Doorgifte van persoonsgegevens

☒ geen doorgifte

©Legal Office WKB